PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-187012
(43)Date of publication of application : 09.07.1999

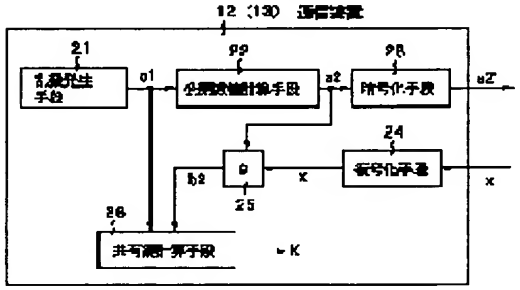
(51)Int.Cl. H04L 9/08
G09C 1/00
H04L 9/32

(21)Application number : 09-352964
(22)Date of filing : 22.12.1997

(71)Applicant : NEC CORP
(72)Inventor : MURAKAMI TAKUYA

(54) SHARED KEY EXCHANGING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a shared key exchanging system with which a shared key can be exchanged safely without requiring previous cryptographic key generation/exchange for certification between respective pieces of communication equipment.



SOLUTION: Two pieces of communication equipment for performing cryptographic communication encipher a disclosed numerical value generated by their own disclosed numerical coefficient means 22 through an enciphering means 23 while using the disclosed key of a managing center and transmit it to the managing center. The managing center deciphers this numerical value while using its own secret key and after two disclosed numerical values of two pieces of communication equipment are provided, the deciphered disclosed numerical value and a prescribed function enciphered while using its own secret key are transmitted to two pieces of communication equipment for performing cryptographic communication. Every communication equipment performs certification by deciphering the received value through a deciphering means 24 while using the disclosed key of the managing center, provides a deciphered value, calculates a function (g) from that deciphered value and its own disclosed numerical value and further calculates the shared key through a shared key calculating means 26 while using a random number.

LEGAL STATUS

[Date of request for examination] 22.12.1997

[Date of sending the examiner's decision of rejection] 09.01.2001

[Kind of final disposal of application other than the examiner's decision of rejection or

application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－187012

(43)公開日　平成11年(1999)７月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｄ
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ　1/00	６３０Ｅ
			６３０Ｄ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６０１Ｅ
			６７５Ｄ

審査請求　有　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願平9－352964

(22)出願日　平成９年(1997)12月22日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　村上　卓弥
東京都港区芝５丁目７番１号　日本電気株式会社内

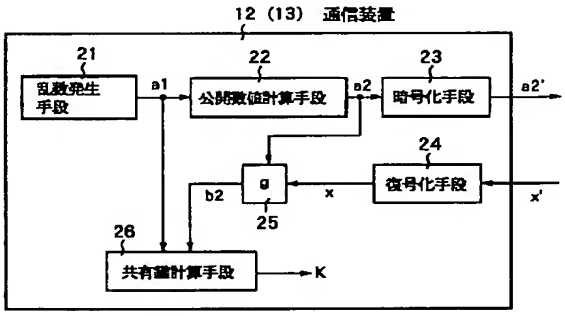
(74)代理人　弁理士　松浦　兼行

(54)【発明の名称】　共有鍵交換方式

(57)【要約】

【課題】　管理センタを使用しないブ従来方式では、第三者へ通信の秘密が漏洩する可能性が高い。管理センタを使用する従来方式では、暗号通信を開始する前に予め暗号鍵生成・配送を別に行っておかなければならず、利便性が悪い。

【解決手段】　暗号通信を行う２つの通信装置は、自身の公開数値係数手段２２で生成した公開数値を、暗号化手段２３において管理センタの公開鍵を用いて暗号化し、管理センタに送信する。管理センタではこれを自身の秘密鍵を使って復号化し、２つの通信装置の２つの公開数値を得た後、復号公開数値と自身の秘密鍵を用いて暗号化した所定の関数を暗号通信を行う２つの通信装置へ送信する。各通信装置は受信した値を管理センタの公開鍵を使って復号化手段２４で復号化することで認証を行うと共に復号値を得て、その復号値と自身の公開数値とから関数ｇを計算し、更に乱数を用いて共有鍵計算手段２６で共有鍵を計算する。



1

【特許請求の範囲】

【請求項１】　管理センタが公開鍵の生成を行い暗号通信を行う複数の通信装置に配布し、これら複数の通信装置間で共有鍵を交換する共有鍵交換方式において、

前記複数の通信装置のうち暗号通信を行う２つの通信装置は、それぞれ公開数値と秘密数値を生成し、前記管理センタの公開鍵を用いて暗号化して前記管理センタへ送信する暗号送信手段と、前記管理センタの送信信号を受信して前記公開鍵を用いて復号化することで認証を行うと共に復号値を得る第１の復号化手段と、自身の前記公開数値と秘密数値と前記第１の復号化手段よりの復号値とに基づき共有鍵を計算する計算手段とを備え、

前記管理センタは、前記暗号通信を行う２つの通信装置から送信された前記暗号を受信し、自身の秘密鍵を用いて前記２つの通信装置の公開数値をそれぞれ復号する第２の復号化手段と、前記第２の復号化手段からの復号公開数値と自身の秘密鍵を用いて暗号化した所定の関数を前記暗号通信を行う２つの通信装置へ送信する送信手段とを備えることを特徴とする共有鍵交換方式。

【請求項２】　前記２つの通信装置のそれぞれの暗号送信手段は、乱数を前記秘密数値として発生する乱数発生手段と、前記秘密数値に基づいて前記公開数値を計算する公開数値計算手段と、前記公開数値計算手段からの公開数値を前記管理センタの公開鍵を用いて暗号化して前記管理センタへ送信する第１の暗号化手段とからなり、

前記計算手段は、前記第１の復号化手段からの復号値と前記公開数値計算手段からの公開数値とから相手の通信装置の公開数値を計算する第１の計算手段と、前記第１の計算手段により計算された公開数値と自身の前記乱数発生手段からの秘密数値とに基づいて共有鍵を計算する共有鍵計算手段とからなることを特徴とする請求項１記載の共有鍵交換方式。

【請求項３】　前記管理センタの送信手段は、前記第２の復号化手段からの復号公開数値と自身の秘密鍵を用いて前記所定の関数を計算する関数計算手段と、前記所定の関数を前記管理センタの秘密鍵を用いて暗号化して前記暗号通信を行う２つの通信装置へ送信する第２の暗号化手段とからなることを特徴とする請求項１記載の共有鍵交換方式。

【請求項４】　前記管理センタは複数あり、複数の通信装置のうち暗号通信を行う２つの通信装置とこれら複数の管理センタそれぞれの間で複数の共有鍵を生成し、これら複数の共有鍵すべてを用いて一つの共有鍵を生成することを特徴とする請求項１記載の共有鍵交換方式。

【請求項５】　前記一つの共有鍵の生成は、前記複数の共有鍵をそれぞれビット毎の排他的論理和演算により計算して行うことを特徴とする請求項４記載の共有鍵交換方式。

【請求項６】　前記暗号通信を行う２つの通信装置の暗号送信手段は、ディフィー・ヘルマン・キー・アグリーメント・プロトコルにより前記公開数値と秘密数値を生成し、前記計算手段は自身の前記公開数値と秘密数値と前記第１の復号化手段よりの復号値とに基づきディフィー・ヘルマン・キー・アグリーメント・プロトコルにより共有鍵を計算することを特徴とする請求項１記載の共有鍵交換方式。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は共有鍵交換方式に係り、特に暗号通信を行う通信装置間で共有鍵暗号化方式を用いて共有鍵を交換する共有鍵交換方式に関する。

【０００２】

【従来の技術】通信装置の間で秘密情報の通信を安全に行うためには、暗号を用いる通信が有効である。暗号の方法には、共有鍵暗号化方式と公開鍵暗号化方式とがある。共有鍵暗号化方式は、暗号通信を行う通信装置の間で共通の鍵を用いる方式で、例えばデータ暗号化規格のＤＥＳ暗号がある（"Data Encryption Standard",FIPSPublication 46,National Institute of Standards and Technolpgy(NIST),1993）。公開鍵暗号化方式は、秘密鍵と公開鍵の２つの鍵を用いる方式で、例えばＲＡＳ暗号がある（"A Method for obtaining digital signatures and publickeycryptosystems",R.L.Rivest,A.Shamir,and L.M.Adleman.Communications of the ACM,21(2),February 1978 ）。

【０００３】共有鍵暗号化方式では、共有鍵を暗号通信を行う通信装置間で交換することが必要であり、管理センタが鍵の生成を行い配布を行う方法と、管理センタを必要としない方法（例えば、Diffie-Hellman key agreement protocol("New directions in cryptography",W.Diffie and M.E.Hellman,IEEE Transactions on Information Theory,IT-22:644-654,1976) ）が開示されている。

【０００４】上記のプロトコル（Diffie-Hellman key agreement protocol)では、第三者が暗号通信を行う通信装置間に割り込むことで通信の秘密が漏洩する可能性がある。具体的には、通信装置から別の通信装置に共有鍵交換のための情報を送信する際、伝送路上の第三者がこの情報を横取りし、偽造情報にすり替えて送信することで鍵交換に割り込み、共有鍵不正に取得することが可能である。

【０００５】これを防止するため、通信装置間で認証を行うプロトコル（Authenticated Diffie-Hellman key agreement protocol)が知られている（"Authentication andauthenticated key exchanges",W.Diffe,P.C.Van Oorschot,and M.J.Wiener,Designs,Codes and Cryptography,2:107-125,1992）。このプロトコルでは、鍵交換を行う各通信装置上で認証のための鍵を事前に生成しておく必要がある。

【０００６】管理センタを用いる方法では、管理センタ

の認証情報を用いる共有鍵配送方式が知られている（特開平２－２４６６４０号公報）。この従来方式でも、各通信装置間で認証が行われるため、第三者が鍵交換に割り込むことがない。この従来方式では、まず、管理センタと各通信装置の間で秘密鍵を生成して共有しておく。その後、一つの通信装置の依頼により管理センタは、その通信装置と指定された通信装置との相互の認証に必要な情報を生成し、その情報を依頼元の通信装置及び指定の通信装置に、秘密情報を用いた秘密通信により送信する。

【０００７】そして、相互認証に必要な情報を得た複数の通信装置が共有鍵の配送を行うときに、二重暗号演算装置を用いて共有鍵の配送を行うと共に、互いに相手側の通信装置の正当性を管理センタから得た情報を用いて相互に認証する。

【０００８】

【発明が解決しようとする課題】しかるに、上記の共有鍵交換方式のうち、管理センタを使用しないで共有鍵を暗号通信を行う通信装置間で交換するプロトコル（Diffie-Hellman key agreement protocol)では、第三者へ通信の秘密が漏洩する可能性が高いということである。その理由は、各通信端末間の認証がないため、第三者が各通信端末間の通信に割り込むことが可能なためである。

【０００９】一方、上記の管理センタを使用しないプロトコル（Diffie-Hellman key agreement protocol)以外の従来の共有鍵交換方式では、共有鍵の交換において安全性は確保されるが、暗号通信を開始する前に予め暗号化・認証のための暗号鍵生成・配送を別に行っておかなければならないため、利便性が損なわれるということである。その理由は、第三者への秘密通信の漏洩を防ぐため、認証情報を事前に用意し、各通信装置間の認証を行わなければならないためである。

【００１０】本発明は以上の点に鑑みなされたもので、共有鍵暗号化方式において、各通信装置で認証のための事前の暗号鍵生成・交換を必要とせずに共有鍵を安全に交換し得る共有鍵交換方式を提供することを目的とする。

【００１１】また、本発明の他の目的は、従来方式に比べて第三者へ通信の秘密が漏洩する可能性が低く、また、各通信装置での認証のための事前の暗号鍵生成・交換の手続き及び管理センタへの登録を不要にし得る共有鍵交換方式を提供することにある。

【００１２】

【課題を解決するための手段】上記の目的を達成するため、本発明は管理センタが公開鍵の生成を行い暗号通信を行う複数の通信装置に配布し、これら複数の通信装置間で共有鍵を交換する共有鍵交換方式において、複数の通信装置のうち暗号通信を行う２つの通信装置は、それぞれ公開数値と秘密数値を生成し、管理センタの公開鍵を用いて暗号化して管理センタへ送信する暗号送信手段

と、管理センタの送信信号を受信して公開鍵を用いて復号化することで認証を行うと共に復号値を得る第１の復号化手段と、自身の公開数値と秘密数値と第１の復号化手段よりの復号値とに基づき共有鍵を計算する計算手段とを備え、管理センタは、暗号通信を行う２つの通信装置から送信された暗号を受信し、自身の秘密鍵を用いて２つの通信装置の公開数値をそれぞれ復号する第２の復号化手段と、第２の復号化手段からの復号公開数値と自身の秘密鍵を用いて暗号化した所定の関数を暗号通信を行う２つの通信装置へ送信する送信手段とを備える構成としたものである。

【００１３】ここで、２つの通信装置のそれぞれの暗号送信手段は、乱数を秘密数値として発生する乱数発生手段と、秘密数値に基づいて公開数値を計算する公開数値計算手段と、公開数値計算手段からの公開数値を管理センタの公開鍵を用いて暗号化して管理センタへ送信する第１の暗号化手段とからなり、計算手段は、第１の復号化手段からの復号値と公開数値計算手段からの公開数値とから相手の通信装置の公開数値を計算する第１の計算手段と、第１の計算手段により計算された公開数値と自身の乱数発生手段からの秘密数値とに基づいて共有鍵を計算する共有鍵計算手段とからなる。

【００１４】また、上記の管理センタの送信手段は、第２の復号化手段からの復号公開数値と自身の秘密鍵を用いて所定の関数を計算する関数計算手段と、所定の関数を管理センタの秘密鍵を用いて暗号化して暗号通信を行う２つの通信装置へ送信する第２の暗号化手段とからなる。

【００１５】本発明では、暗号通信を行う２つの通信装置は、自身で生成した公開数値を管理センタの公開鍵を用いて暗号化し、管理センタに送信する。管理センタではこれを自身の秘密鍵を使って復号化し、２つの通信装置の２つの公開数値を得た後、復号公開数値と自身の秘密鍵を用いて暗号化した所定の関数を暗号通信を行う２つの通信装置へ送信する。各通信装置は受信した値を管理センタの公開鍵を使って復号化することで認証を行うと共に復号値を得て、その復号値と自身の公開数値と秘密数値とに基づき共有鍵を計算する。

【００１６】従って、上記の公開数値は、各通信装置から管理センタへの送信では暗号化されるため、第三者がこの内容を知ることはできない。また、管理センタから各通信装置への送信においては、公開数値ではなく関数を使って計算した値が送信されるため、関数を適当に選定することにより元の公開数値を第三者が推測することはほぼ不可能である。また、管理センタから各通信装置への送信は、管理センタにより認証されるため、管理センタ以外の第三者が管理センタと各通信装置間野通信に割り込んで偽造情報にすり替えて送信することは不可能である。

【００１７】また、事前の準備は管理センタ側での公開

鍵、秘密鍵の生成のみが必要で、共有鍵の交換の前に各通進端末では認証・暗号化のための暗号鍵の生成及び交換を一切不要にできる。

【００１８】また、本発明は管理センタは複数あり、複数の通信装置のうち暗号通信を行う２つの通信装置とこれら複数の管理センタそれぞれの間で複数の共有鍵を生成し、これら複数の共有鍵すべてを用いて一つの共有鍵を生成するようにしたものである。この発明では、複数の管理センタが同時に使用されて初めて一つの共有鍵を生成する。

【００１９】

【発明の実施の形態】次に、本発明の実施の形態について図面と共に説明する。図１は本発明になる共有鍵交換方式の第１の実施の形態のブロック図を示す。同図に示すように、この実施の形態は、管理センタ１１、第１の通信装置１２及び第２の通信装置１３から構成されている。管理センタ１１は共有鍵交換の仲介を行う装置であり、通信装置１２と通信装置１３は、秘密通信を行う通信装置である。

【００２０】図２は通信装置１２及び１３の一実施の形態のブロック図を示す。通信装置１２及び１３はそれぞれ同一構成で、図２に示すように、乱数発生手段２１、公開数値計算手段２２、暗号化手段２３、復号化手段２４、関数ｇ計算手段２５及び共有鍵計算手段２６より構成されており、共有鍵計算手段２６から共有鍵Ｋを出力する。

【００２１】乱数発生手段２１は乱数を発生するための手段である。公開数値計算手段２２は、乱数発生手段２１から与えられた乱数から公開数値を計算する手段である。暗号化手段２３は、公開数値計算手段２２から与えられた値を管理センタ１１の公開鍵を用いて暗号化する手段である。復号化手段２４は、管理センタ１１から受信した値を管理センタ１１の公開鍵を用いて復号化し、認証を行う手段である。関数ｇ計算手段２５は、公開数値計算手段２２と復号化手段２４から与えられた値を関数ｇに適用した値を計算する手段である。共有鍵計算手段２５は、乱数発生手段２１と関数ｇ計算手段２５から与えられた数値から共有鍵Ｋを計算する手段である。関数ｆ、ｇはｙ＝ｇ（ｘ，ｆ（ｘ，ｙ））を満たすように選ぶ。

【００２２】図３は管理センタ１１の一実施の形態のブロック図を示す。管理センタ１１は復号化手段３１、関数ｆ計算手段３２及び暗号化手段３３からなる。復号化手段３１は、通信装置１２及び１３から与えられた数値を、管理センタ１１の秘密鍵を用いて復号化する手段である。関数ｆ計算手段３２は、復号化手段３１から与えられた数値を関数ｆに適用した値を計算する手段である。暗号化手段３３は、関数ｆ計算手段３２から与えられた値を、管理センタ１１の秘密鍵を用いて暗号化・署名する手段である。

【００２３】次に、図１、図２及び図３と共に本発明の実施の形態の動作について説明する。まず、記法を説明する。ｘ，ｙを任意の整数とするとき、ｘ＊ｙはｘとｙの乗算を表す。ｅｘｐ（ｘ，ｙ）は、ｘのｙ乗を表す。また、ｘ　ｍｏｄｅ　ｙは、ｘについてのｙを法とする剰余を表す。また、ｘ　ＸＯＲ　ｙは、ｘ，ｙを２進数とみなしたときのｘとｙのビット毎の排他的論理和を表す。

【００２４】（１）ステップ１

一方の通信装置１２は、乱数発生手段２１により乱数ａ１を発生する。公開数値計算手段２２はこの乱数ａ１に基づいて公開数値ａ２を計算する。暗号化手段２３はこの公開数値ａ２を管理センタ１１の公開鍵を用いて暗号化して暗号ａ’を計算し、その暗号ａ’を管理センタ１１に送信する。同様に、他方の通信装置１３は、乱数ｂ１を発生して公開数値ｂ２を計算し、これと管理センタ１１の公開鍵に基づき暗号ｂ２’を計算して管理センタ１１に送信する。

【００２５】（２）ステップ２

管理センタ１１は、図３の復号化手段３１により管理センタ１１の秘密鍵を用いて、暗号ａ２’及びｂ２’を復号化し、公開数値ａ２及びｂ２を計算した後、これらａ２及びｂ２に基づいて関数ｆ計算手段３２によりｘ＝ｆ（ａ２，ｂ２）を計算する。続いて、管理センタ１１は、その関数ｆを暗号化手段３３において秘密鍵を用いて暗号化し、暗号ｘ’を計算して通信装置１２及び１３へそれぞれ送信する。

【００２６】（３）ステップ３

通信装置１２は、管理センタ１１から受信した上記の暗号ｘ’を図２の復号化手段２４で受け、ここで管理センタ１１の公開鍵を用いて関数ｆを復号し、同時に管理センタ１１の認証を行う。続いて、通信装置１２内の関数ｇ計算手段２５は、復号された関数ｆの値ｘ（＝ｆ（ａ２，ｂ２））と、公開数値計算手段２２からの公開数値ａ２とに基づいて、関数ｇ（ａ２，ｘ）を計算する。ここで、任意のｘ，ｙの値に対し、ｙ＝ｇ（ｘ，ｆ（ｘ，ｙ））となるように、ｆ，ｇを選んであるので、ｇ（ａ２，ｘ）＝ｇ（ａ２，ｆ（ａ２，ｂ２））＝ｂ２となり、通信装置１３で計算された公開数値ｂ２が関数ｇ計算手段２５により得られる。次に、関数ｇ計算手段２５により得られた公開数値ｂ２と、乱数発生手段２１で発生された乱数ａ１とに基づいて、共有鍵計算手段２６は共有鍵Ｋを計算する。

【００２７】同様に、通信装置１３は、管理センタ１１から受信した暗号ｘ’から関数ｆを復号し、その復号値と内部の公開数値計算手段からの公開数値ｂ２を用いて関数ｇを計算することで、ｇ（ｂ２，ｘ）＝ｇ（ｂ２，ｆ（ａ２，ｂ２））＝ａ２を得て、これと内部の乱数発生手段で発生した乱数ｂ１とから共有鍵Ｋを計算する。

【００２８】次に、本発明の第２の実施の形態について

説明する。図４は本発明の第２の実施の形態のブロック図を示す。同図において、第１の通信装置４１と第２の通信装置４２の間に、ｎ個の管理センタ４３$_1$～４３$_n$から構成されている。

【００２９】第１の実施の形態では、暗号化と署名により管理センタ以外の第三者が鍵交換に割り込んで鍵交換のための情報を偽造情報にすり替えることは不可能であるが、管理センタ１１が通信装置１２と通信装置１３の伝送路の途中にある場合、管理センタ１１自体が鍵交換に割り込んで情報を偽造情報にすり替えることは可能である。そのため、管理センタ１１が十分に信用できない場合は、通信装置１２と通信装置１３の間の秘密通信が管理センタ１１に漏洩する危険性がある。

【００３０】そこで、この第２の実施の形態では、複数の管理センタ４３$_1$～４３$_n$を用いてこの危険性を低下させるようにしたものである。すなわち、この第２の実施の形態の動作について説明するに、まず、管理センタ４３$_1$を用いて第１の実施の形態と同様に、通信装置４１と通信装置４２の間で共有鍵Ｋ１を生成する。次に、管理センタ４３$_2$を用いて共有鍵Ｋ２を生成する。

【００３１】以下、上記と同様にして、管理センタ４３$_3$～４３$_n$をそれぞれ順次に使用して共有鍵Ｋ３、．．．、Ｋｎを生成する。最後に、これらすべての共有鍵Ｋ１～Ｋｎを用いて共有鍵Ｋを計算する。この共有鍵Ｋの計算には、ビット毎の排他的論理和を用いて、Ｋ＝Ｋ１ ＸＯＲ Ｋ２ ＸＯＲ ．．． ＸＯＲ Ｋｎにより計算する方法がある。

【００３２】第２の実施の形態では、ｎ個のすべての管理センタ４３$_1$～４３$_n$が結託して鍵交換に割り込まない限り、通信装置４１と４２の間の秘密通信が漏洩することはないため、安全性が向上する。

【００３３】

【実施例】次に、本発明の一実施例について説明する。公開鍵暗号化方式としてＲＳＡ暗号化方式を用いることとする。管理センタの公開鍵を（ｎ，ｅ）、秘密鍵を（ｎ，ｄ）とすると、暗号化手段２３での演算は、ａ２’＝ｅｘｐ（ａ２，ｅ） ｍｏｄ ｎとなり、復号化手段２４での演算は、ｘ＝ｅｘｐ（ｘ’，ｅ） ｍｏｄ ｎとなる。また、復号化手段３１での演算はａ２＝ｅｘｐ（ａ２’，ｄ） ｍｏｄ ｎ、ｂ２＝ｅｘｐ（ｂ２’，ｄ） ｍｏｄ ｎとなり、暗号化手段３３での演算はｘ’＝ｅｘｐ（ｘ，ｄ） ｍｏｄ ｎとなる。

【００３４】公開値計算、共有鍵計算のアルゴリズムは、前記のディフィー・ヘルマン・キー・アグリーメント・プロトコル（Diffie-Hellmann key agreement protocol：以下、従来のプロトコルという）を用いる。この方法では、２つのアルゴリズムパラメータｐ，ｇを必要とする。ここで、ｐは素数であり、ｇはｐ以下の整数で、ｇを整数倍してｐで剰余をとった値として、１からｐ－１までのすべての整数を生成できる数値である。このとき、公開数値計算手段２２での演算は、ａ２＝ｅｘｐ（ｇ，ａ１） ｍｏｄ ｐとなる。また、共有鍵計算手段２６での演算はＫ＝ｅｘｐ（ｅｘｐ（ｇ，ｂ２），ａ１） ｍｏｄ ｐとなる。

【００３５】ｐ，ｇは事前に通信装置１２と通信装置１３の間で共有しておく必要があるが、この値自身は公開してもよいもので、通常の通信回線を用いて通信端末１２と通信端末１３の間で合意すればよい。また、関数ｆ（ｘ，ｙ）及びｇ（ｘ，ｙ）は、任意の整数ｘ，ｙについて、ｙ＝ｇ（ｘ，ｆ（ｘ，ｙ））を満たす必要がある。ここでは、ｆ（ｘ，ｙ）＝ｇ（ｘ，ｙ）＝ｘ ＸＯＲ ｙとする。

【００３６】次に、この実施例の動作について説明する。

【００３７】（１）ステップ１

通信装置１２は、従来のプロトコルで使用するシステムパラメータｐ，ｇを生成する。これを通信装置１３に送信し、共有しておく。

【００３８】（２）ステップ２

通信装置１２は、乱数発生手段２１により乱数ａ１を生成する。次に、公開数値計算手段２２により公開数値ａ２をｅｘｐ（ｇ，ａ１） ｍｏｄ ｐなる式により計算し、管理センタ１１の公開鍵（ｎ，ｅ）を用いて暗号化手段２３で暗号ａ２’をｅｘｐ（ａ２，ｅ） ｍｏｄ ｎにより計算した後、管理センタ１１にａ２’を送信する。同様に、通信装置１３は乱数ｂ１を生成し、公開数値ｂ２をｅｘｐ（ｇ，ｂ１） ｍｏｄ ｐなる式により計算し、管理センタ１１の公開鍵（ｎ，ｅ）を用いて暗号ｂ２’をｅｘｐ（ｂ２，ｅ） ｍｏｄ ｎにより計算した後、管理センタ１１にｂ２’を送信する。

【００３９】（３）ステップ３

管理センタ１１は、管理センタ１１の秘密鍵（ｎ，ｄ）と復号化手段３１を用いて、ａ２’及びｂ２’を復号化し、ａ２＝ｅｘｐ（ａ２’，ｄ） ｍｏｄ ｐ、ｂ２＝ｅｘｐ（ｂ２’，ｄ） ｍｏｄ ｎを計算する。これと関数ｆ計算手段３２を用いて、ｘ＝ａ２ ＸＯＲ ｂ２を計算する。これを管理センタ１１の秘密鍵を用いて暗号化手段３３により暗号化し、ｘ’＝ｅｘｐ（ｘ，ｄ） ｍｏｄｎを計算し、その計算結果ｘ’を通信装置１２及び通信装置１３へ送信する。

【００４０】（４）ステップ４

通信装置１２は、管理センタ１１から受信したｘ’から管理センタ１１の公開鍵を用いて復号化手段２４により、ｘ＝ｅｘｐ（ｘ’，ｅ） ｍｏｄ ｎを計算し、同時に管理センタ１１の認証を行う。次に、通信装置１２は、計算したｘと、公開数値ａ２の値から、関数ｇ計算手段２５によりａ２ ＸＯＲ ｘ＝ａ２ＸＯＲ （ａ２ ＸＯＲ ｂ２）＝ｂ２を計算する。次に、得られたｂ２と乱数ａ１の値から、共有鍵計算手段２６によりｅｘｐ（ｂ２，ａ１） ｍｏｄ ｐ＝ｅｘｐ（ｅｘｐ（ｇ，

ｂ１），ａ１）　ｍｏｄ　ｐ＝ｅｘｐ（ｇ，ａ１＊ｂ１）ｍｏｄ　ｐ＝Ｋを計算して、共用鍵Ｋを得る。

【００４１】一方、通信装置１３も同様にして、管理センタ１１から受信したｘ’から管理センタ１１の公開鍵を用いて、復号化手段によりｘ＝ｅｘｐ（ｘ’，ｅ）ｍｏｄ　ｎを計算し、同時に管理センタ１１の認証を行う。次に、通信装置１３は、計算したｘと、公開数値ｂ２の値から、関数ｇ計算手段によりｂ２　ＸＯＲ　ｘ＝ｂ２　ＸＯＲ　（ａ２　ＸＯＲ　ｂ２）＝ａ２を計算する。次に、得られたａ２と乱数ｂ１の値から、共有鍵計算手段によりｅｘｐ（ａ２，ｂ１）　ｍｏｄｐ＝ｅｘｐ（ｅｘｐ（ｇ，ａ１），ｂ１）　ｍｏｄ　ｐ＝ｅｘｐ（ｇ，ａ１＊ｂ１）　ｍｏｄ　ｐ＝Ｋを計算して、共用鍵Ｋを得る。

【００４２】

【発明の効果】以上説明したように、本発明によれば、管理センタと各通信装置の間の通信が暗号化、認証されるため、管理センタ以外の第三者が鍵交換に割り込むことが不可能であり、また、第三者は公開数値を知ることもできず、共有鍵を推測することが極めて困難であるため、従来の管理センタを使用しない共有鍵交換方式（ディフィー・ヘルマン・キー・アグリーメント・プロトコル：Diffie-Hellmann key agreement protocol）に比べて、第三者へ通信の秘密が漏洩する可能性が低く、この結果、従来に比べてセキュリティを向上できる。

【００４３】また、本発明によれば、管理センタ側の鍵を用いた公開鍵暗号化方式を用いて暗号通信、認証を行うことにより、各通信装置側では鍵生成が不要なため、＊＊従来に比べて、通信端末側の事前の鍵生成・交換の手続き、及び管理センタの登録が不要にでき、保守性を向上できる。

【００４４】更に、本発明によれば、管理センタを複数設け、それぞれに共有鍵を生成させた後、これら複数の共有鍵から共有鍵を計算するようにしたため、複数あるすべての管理センタが結託して鍵交換に割り込まない限り、通信装置間の秘密通信が漏洩することがなく、管理センタが単一の場合よりも、より一層安全性を向上できる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態のブロック図である。

【図２】図１中の通信装置の一例のブロック図である。

【図３】図１中の管理センタの一例のブロック図である。

【図４】本発明の第２の実施の形態のブロック図である。

【符号の説明】

１１、４３$_1$～４３$_n$　管理センタ

１２、１３、４１、４２　通信装置

２１　乱数発生手段

２２　公開数値計算手段

２３、３３　暗号化手段

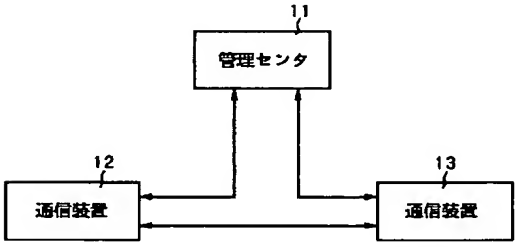
２４、３１　復号化手段

２５　関数ｇ計算手段

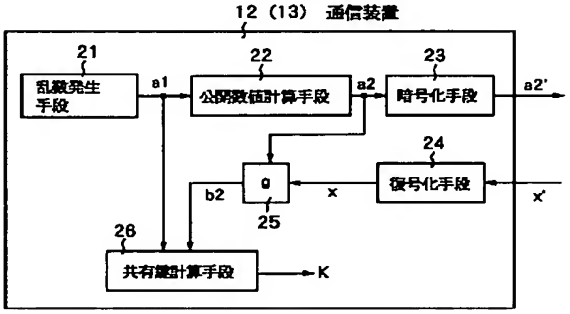
２６　共有鍵計算手段

３２　関数ｆ計算手段

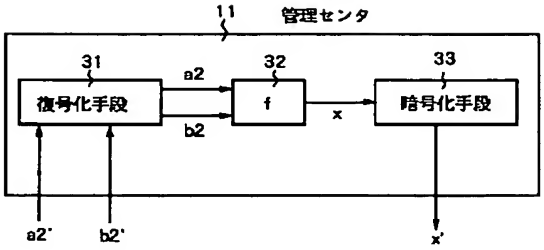
【図１】



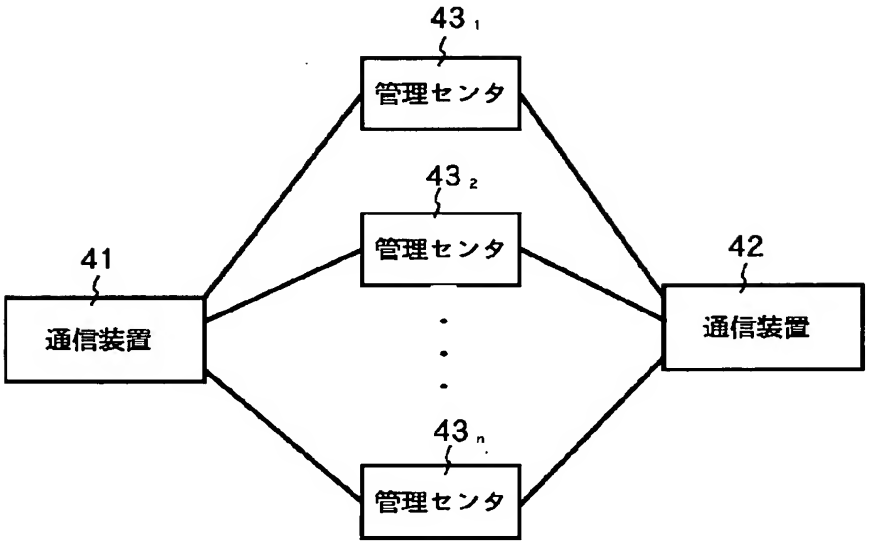
【図２】



【図３】


11
管理センタ
31
32
33
a2
b2
復号化手段
f
x
暗号化手段
a2'
b2'
x'

【図４】


43 1
管理センタ
43 2
管理センタ
41
42
通信装置
通信装置
43 n
管理センタ